Pre-Processing Power Traces with a Phase-Sensitive Detector

Pre-Processing Power Traces with a Phase-Sensitive Detector

P. Hodgers, N. Hanley, M. O'Neill
Centre for Secure Information Technologies
Queens University Belfast, United Kingdom
p.hodgers@qub.ac.uk, n.hanley@qub.ac.uk, m.oneill@ecit.qub.ac.uk

Abstract — **As cryptographic implementations are increasingly subsumed as functional blocks within larger systems on chip, it becomes more difficult to identify the power consumption signatures of cryptographic operations amongst other unrelated processing activities. In addition, at higher clock frequencies, the current decay between successive processing rounds is only partial, making it more difficult to apply existing pattern matching techniques in side-channel analysis. We show however, through the use of a phase-sensitive detector, that power traces can be pre-processed to generate a filtered output which exhibits an enhanced round pattern, enabling the identification of locations on a device where encryption operations are occurring and also assisting with the re-alignment of power traces for side-channel attacks.**

Keywords; side-channel attack, phase-sensitive detector, cartography.

I. INTRODUCTION

Cryptographic functions are increasingly incorporated into embedded devices such as mobile phones and other portable computing devices to enhance security. Although encryption offers a high level of theoretical security for the data that is stored on the device, the underlying hardware that implements the encryption algorithms has been shown to leak side-channel information. This side-channel information can be recorded through the use of probes connected to a device's internal circuitry, or through less invasive means such as with a non-contact electro-magnetic probe. The gathered data can then be statistically processed to uncover the key that secures the underlying encryption algorithm and thus enables the decryption of all data previously encrypted with the same key. These threats are not just of theoretical interest, but reflect vulnerabilities in real-world devices as illustrated in [18, 20].

In order to mount a successful side-channel attack, an attacker needs to obtain a set of well-aligned power consumption traces. Devices running various concurrent operations may process encryption routines in varying time segments. Measurements taken from real world devices will also seldom have a readily available trigger source to synchronise the extraction of the power waveform data. This is required since an attacker will want to compare the same point in time for each encryption operation. Misalignments may also be intentionally introduced as a countermeasure in the form of random delay insertions [21]. These factors contribute to make it more difficult for an attacker to successfully gather the power traces and also to identify the target cryptographic processing sequences from within the side-channel data. The first contribution of this paper is to introduce the novel application of a phase-sensitive detector to enhance power traces for realignment and side-channel attacks.

Power analysis traces are generally recorded with an oscilloscope, measuring the supply voltage drop across a load resistor, and consist of the macro level power consumptions of the device. Although the trace captures the encryption related processing power, it will also consist of the contributions from other concurrent processing activities, effectively adding noise to the signal. The power traces also contain a certain amount of electronic, algorithmic and quantisation noise that will vary between successive acquisitions. This noise effect can be overcome to a certain extent through the use of filtering to improve the signal to noise ratio and through the averaging of large numbers of traces in the statistical analysis.

Another source of side-channel information is electro-magnetic emanation. Here an attacker typically uses a less invasive near-field sensing probe, with the aim of extracting power consumption signatures that are more localised to the encryption processing whilst reducing contributions from other unrelated regions of the device. The question then arises as to where the probe should be placed to gain the optimal data for the attack? Side-channel cartography is a technique that can assist with answering this question by enabling the precise placement of a probe across the surface of a device under control of a scanning platform. Our second contribution is to demonstrate how the phase-sensitive detector can also be used to perform a pattern extraction to quickly identify areas of the device that contain the encryption signature and thus represent advantageous locations for focusing the gathering of side-channel information.

This paper is organised as follows; Section II provides background information and discusses previous research in the area of side-channel attacks. Section III describes the phase-sensitive detector filtering method we are proposing. Section IV details the experimental setup and presents results for the re-alignment and correlation power analysis (CPA) attack on an FPGA implementation of the AES algorithm. We then demonstrate how the phase-sensitive detector technique can be extended to characterise an encryption signature and use this to identify relevant regions of electromagnetic emanation in a cartography analysis of an FPGA device.

II. BACKGROUND AND PREVIOUS RESEARCH

A. Side Channel Attacks

Side Channel Attack (SCA) techniques were first published by Kocher *et al.* [1], with a timing analysis of exponentiation operations in a cryptographic device and subsequently through the technique of Differential Power Analysis (DPA) [2]. Later this research was expanded by Quisquater *et al.* in dealing with electromagnetic (EM) waveforms in Differential Electro-

magnetic Analysis (DEMA) [3], with further experimental results published by Gandolphi *et al.* [4] and Agrawal *et al.* [5].

In these attacks, the measurements capture a time domain representation of the power consumption during a cryptographic operation. This power consumption can be compared against a modeled set of hypothetical power consumption values via a statistical analysis such as the Pearson correlation coefficient, as introduced by Brier *et al.* with Correlation Power Analysis (CPA) [6]. Let the correlation, $\rho_{x,y}$ be a function of the hypothetical power model, H, and the measured power, P, such that;

$$\rho_{H,P} = \frac{\sum(H_i - \bar{H})(P_i - \bar{P})}{\sqrt{\sum(H_i - \bar{H})^2}\sqrt{\sum(P_i - \bar{P})^2}} \quad (1)$$

Where $\bar{H}$ and $\bar{P}$ relate to the mean of the respective hypothetical and measured power data sets and where H_i and P_i refer to the individual hypothetical and measured power trace elements, at a particular instant in time. The reader is referred to [21] for a comprehensive overview on power analysis attacks.

B. Side-Channel Cartography

Side-channel cartography is the multi-dimensional analysis of a device for side-channel attacks. This approach was described by Quisquater *et al.* for Smart Cards [3] and then extended by Sauvage *et al.* to identify side-channel emanation hot-spots in an FPGA [12, 17]. The approach of surface scanning electronic circuits is already widely used in industry for the qualification of circuits for electromagnetic emissions in ISO/IEC standard 61967 [13].

Whilst power analysis data can be simply measured as the time-varying voltage drop across a fixed load resistor, for an electro-magnetic (EM) analysis the attacker usually has a probe that needs to be placed in a suitable position to record localised readings of the electric or magnetic field strength. Problems arise as to where the optimal point to position the probe is, particularly for small probes suitable for high resolution scanning of discrete points across the device, such as the approach described in [12]. Although Sauvage *et al.* used a cross correlation technique to find areas of self-similar emanation in [17], they did not identify whether the locations were emanating encryption related information or not.

C. Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a symmetric block cipher adopted for use as US Federal Information Processing Standard - 197 [7]. AES has a fixed block size of 128 bits, with optional key size usage of 128, 192, and 256 bits. In this paper, the 128 bit key AES implementation is used, which processes 10 intermediate rounds between plaintext input and ciphertext output.

The target for the attack is a specific point in time during the algorithm when it is processing some intermediate value that is data dependant with the secret key. For iterative hardware AES implementations, a suitable location is the register transfer between rounds 9 and 10 allowing us to build a Hamming-distance power model. As the *MixColumn* operation, which operates on 32-bit words, is not present in the final round, the model can be built for 8-bits at a time allowing a decomposition of the key search space from 2^{128} to 16×2^{8}.

D. Filtering to reduce noise and improve pattern recognition

For cryptography running on devices at higher clock speeds the power contributions from each round of processing will tend to merge with each other, as discussed in [21]. As shown in Fig. 1 (a), the AES encryption algorithm running at 2MHz exhibits separate and distinct rounds of processing. It can be observed that the power consumption fully decays back to the background noise level before commencing the next round of processing. In Fig. 1 (b) however, running the same algorithm, but this time at 24MHz, it can be observed that the rounds of processing occur closely together and the power consumption does not have time to decay before the next round of processing. The resultant waveform is a larger single shape with smaller ripple peaks for each round. The processing peaks vary in height between the rounds and also across trace acquisitions, making a cross-correlated pattern extraction of the individual rounds difficult.

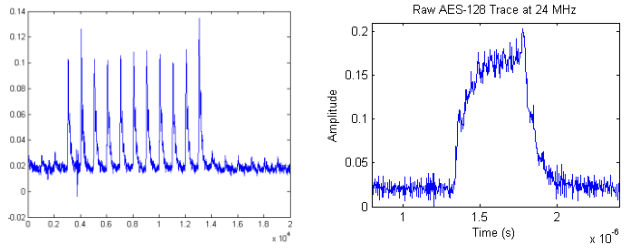

Figure 1. (a) AES encryption operating at 2MHz – the rounds are distinct and well suited to a pattern extraction. (b) Operating at 24MHz – the rounds are now merging, making pattern extraction difficult.

The suitable application of a filter can help to improve the signal-to-noise ratio (SNR) of the data, as well as improving the visual appearance to allow features of interest to be identified for simple power analysis and/or realignment.

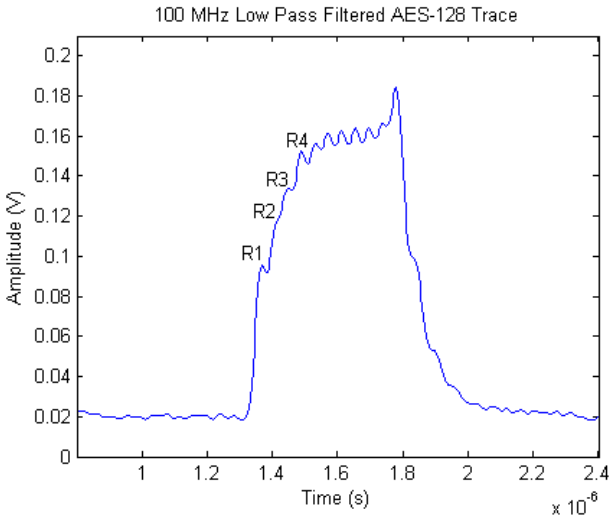

Figure 2. AES encryption filtered at 100 MHz.

By applying a low pass filter, the higher frequency noise components can be attenuated. Fig. 2 shows the result of a 100MHz low pass filter applied to the waveform of Fig. 1 (b).

The individual rounds are now more clearly visible, providing a discernible pattern. However, it is still difficult to do an extraction of the individual rounds due to the large amplitude variation between the rounds and also the difference in amplitude between rounds in successive traces, where on occasion the round may merge into the pattern, such as the second round, highlighted as R2 in Fig. 2.

Barenghi *et al.* also showed that a series of band pass filters can be used to extract the system clock frequency and selected harmonics, where significant side-channel information may be found [11], whilst rejecting other unrelated frequencies.

E. Alignment of Traces

When mounting an attack in the time domain, it is important that the data set is well aligned, so that the same point in the encryption algorithm is occurring at the same data point across the trace set. Misalignment may be caused by lack of a readily available and consistent signal to trigger the scope, or there may be some other activity interrupting the processing flow in the device. Additionally some form of countermeasure that inserts a random delay or dummy data operation could be present in an attempt to thwart an attack. In such cases the traces would need to be pre-processed to obtain the data in a re-aligned format.

Several realignment techniques have been proposed. Integrating a windowed portion of the misaligned traces was proposed by Clavier *et al.* in [19], although this approach also introduces a reduction in the correlation coefficient of the order of the square-root of the window width [21]. Homma *et al*. focused on small, high resolution shifting of traces [8]; however this is unsuitable for dealing with larger shift amounts introduced by longer delays and other processing interruptions. In research by Gebotys *et al*. [9], the data is transformed to the frequency domain, with the phase information then replaced across the data set with the phase of one of the acquisitions chosen at random. The theoretical analysis assumed an idealised, noise free, set of source traces, shifted by an arbitrary amount, and it was acknowledged that there would be a phase error introduced by noise in a real-world signal. Another strategy by Hodgers *et al.* [10], exploits the enhanced swing of the power emanations in an EM attack. Here inter-round boundaries of minimal processing power were identified, permitting the individual rounds to be extracted and re-aligned. However, this method requires that the waveform exhibited a large enough peak-to-trough swing to permit a common threshold level to be established across the trace set. The cross correlation techniques described in [22] are suitable for scenarios where the power consumption patterns are distinct and repeatable; however, as we move to higher processing clock frequencies where the rounds merge into one another, these techniques become less applicable.

III. PHASE-SENSITIVE DETECTOR FILTER

The Fourier series demonstrates that any signal may be decomposed into a sum of sine waves of varying frequency, amplitude and phase. In addition, when sine waves of differing frequency or phase are multiplied together, they will result in a zero averaged value, unless they are of exactly the same frequency and phase, in which case the trigonometric identity of the product of two sinusoids applies. These properties are exploited in a phase-sensitive detector (PSD) circuit, also often referred to as a lock-in amplifier, where an input signal is multiplied with a reference sinusoidal waveform to determine if the input signal contains the reference frequency. The non-matching frequencies are then normally discarded through the use of a steep low pass filter, enabling a low amplitude signal of a chosen frequency carrier to be detected in amongst a larger background noise level.

The magnitude of the PSD, V_{psd}, is the product of two sinusoids and is expressed as;

$$V_{psd} = V_{in}V_{ref}\sin(\omega_{in}t + \theta_{in})\sin(\omega_{ref}t + \theta_{ref}) = \frac{V_{in}V_{ref}}{2}\cos([\omega_{in} - \omega_{ref}]t + \theta_{in} - \theta_{ref}) - \frac{V_{in}V_{ref}}{2}\cos([\omega_{in} + \omega_{ref}]t + \theta_{in} + \theta_{ref}) \quad (2)$$

Where,

V_{in} is the magnitude of the input waveform

V_{ref} is the magnitude of the reference waveform

ω_{in} is the angular frequency of the input waveform

ω_{ref} is the angular frequency of the reference waveform

θ_{in} is the phase of the input waveform

θ_{ref} is the phase of the reference waveform

This reduces down to two AC signals, one difference frequency term $(\omega_{in} - \omega_{ref})$ and another sum frequency term $(\omega_{in} + \omega_{ref})$ [14]. Since $\omega_{in} = \omega_{ref}$ for the chosen frequency, the difference term reduces to $\frac{V_{in}V_{ref}}{2}$, a DC term proportional to the signal amplitude.

At this stage the sum frequency term, $(\omega_{in} + \omega_{ref})$, which is all the input Fourier frequency components that make up the input signal, summed with our reference frequency, are usually removed with a low pass filter. However, in the context of a side-channel attack, it is actually this sum frequency term which is of interest since it contains the relevant side-channel leakage. Rather than filter out the sum frequencies with a low pass filter, if we control the relaxation of the low pass filter's cut-off, we can now control the passing of these summed frequencies through to the signal output. The property of this output is that the amplitudes of the frequencies closely associated with our reference frequency are promoted, thus creating a pattern that accentuates the round peaks. Continued relaxing of the filter will eventually enable all frequency components to pass through, recombining to produce the original input waveform again.

As noted, the input has to be in phase with the reference frequency to generate an output, however if we multiply the same input by a second, separate reference, also at the same frequency but this time 90° out of phase (therefore multiplying with a cosine) we generate a separate output which is orthogonal to the first. We now have two output vectors, known as the in-phase and quadrature components respectively. By computing the resultant magnitude of these orthogonal vectors, the phase dependency is removed and we

no longer need to be concerned with the phase difference between ω_{in} and ω_{ref}. This 'two element' PSD arrangement is shown in Fig. 3. The input waveform initially passes through a high pass filter to remove any DC offset. The signal is then split and passed through the sine and cosine multipliers, before passing through the low pass filters, where the cut-off frequency can be adjusted. The signal components are then squared and summed and then the square root operation applied to deliver the magnitude at the signal output.

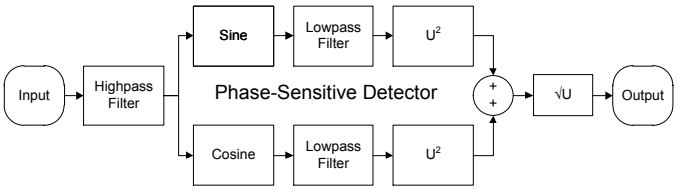

Figure 3. The Phase-Sensitive Detector. Controlling the low pass filter cut-off frequencies enables the manipulation of the output waveform pattern.

The result of adjusting the cut off frequency can be seen in Fig. 4. With a stop frequency of less than 1 MHz, the sum frequency components are mostly filtered out and only the DC term is passed. As the stop frequency is increased to 24 MHz, Fig. 4(a), we can see that some semblance of the waveform shape appears. In Fig. 4(b), the stop frequency is set to 38 MHz, and further sum frequencies are passed, causing the output signal to grow in amplitude and to define the enhanced round pattern. At 48 MHz, Fig. 4(c), the overall amplitude is increased further. Finally setting the stop frequency to 96 MHz, Fig. 4(d), leads to the creation of a pattern that closely resembles the filtered result of Fig. 2. Raising the stop frequency to a high level such as 1GHz, essentially removes the filter effect, with the sum and difference components recombining, outputting the original input waveform. Control of the stop frequency therefore enables us to manipulate the output waveform pattern to better suit a thresholding approach, such as that shown in Fig. 6 (b).

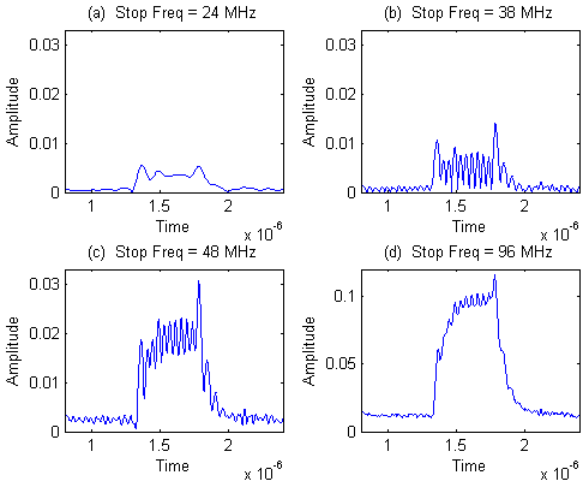

Figure 4. The Phase-sensitive detector processed output with stop frequencies of (a) 24 MHz (b) 38 MHz (c) 48 MHz (d) 96 MHz.

IV. Experimental Results

A. Experimental Setup

We implemented the AES-128 algorithm [7] on a VIRTEX-II FPGA, loading it onto a SASEBO-G side channel attack board [15], running with a clock frequency of 24 MHz. The design is shown in Fig. 6, and is an iterative architecture which computes a complete round every clock cycle. The key is generated in parallel and only the current sub-key is stored in a register. The s-boxes are implemented as asynchronous lookup tables in the slice logic of the FPGA. The design also has a separate feature where AES execution can be randomly delayed through use of liner feedback shift registers to implement a simple random delay countermeasure.

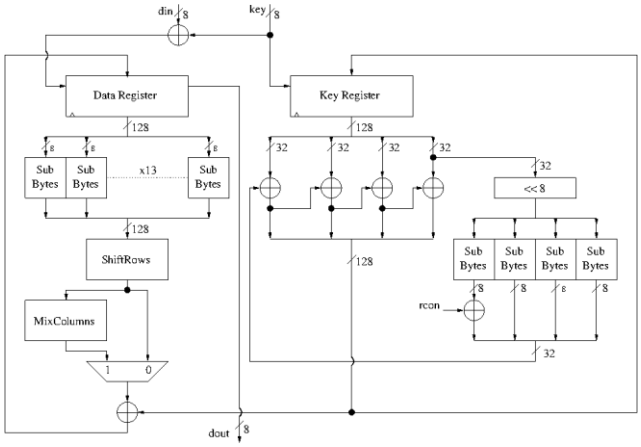

Figure 5. The custom AES-128 implementation loaded onto the SASEBO-G.

A controlling PC was used to send a series of 5000 random plaintexts with a constant key to the AES encryption engine, with an Agilent MSO6104A oscilloscope used to record the trace data at 4GS/s. Each trace was randomly offset from the trigger signal using the random delay insertion feature.

The phase-sensitive detector circuit of Fig. 3 was implemented in MATLAB, with the recorded power traces fed through at the input. The Sine and Cosine references were generated as discrete waveforms using the same sample rate as that for the power traces. The reference frequency was set at 24 MHz and the stop frequency of the low pass filter set to 48MHz, generating the PSD processed output illustrated in Fig. 6 (b).

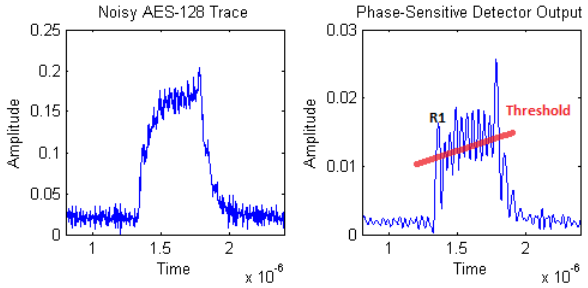

Figure 6. The original waveform (a) was processed through phase-sensitive detector output (b). A threshold was then selected and applied across the data set to extract the round peaks for re-alignment.

The MATLAB *filtfilt* function was used for the low pass filter since this generates a zero-phase digital filter, avoiding the introduction of lag into the PSD response. Note the final large peak in Fig. 6 (b) is due to the power consumption while data is transferred through the FPGA output bus (it is not round 10 of AES). This has no bearing on either the re-alignment, or the subsequent CPA attack as the bus was held low during the round processing.

A thresholding operation was applied, see Fig. 6 (b), to automate the extraction of the round peak positions to enable count across of the rounds and extract the common round peaks positions as a marker for calculating the relative delta. Each trace was then shifted by its delta value from the reference to re-align the trace, as shown in Fig. 7 (a), where the 5000 traces are plotted on top of each other, showing clear alignment.

A correlation attack was then carried out against a single byte of the sub-key in round 10, which successfully revealed the correct key byte of 152, as highlighted in Fig. 7 (b), which shows a plot of all 256 key values. Note that the correlation attack was carried out directly on the PSD output; we did not need to refer back to the original raw trace set. This shows that the PSD output retains the important side-channel information.

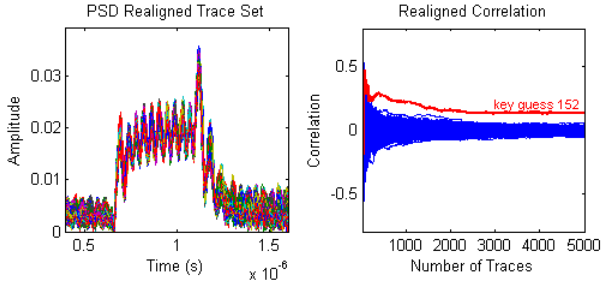

Figure 7. (a) The 5000 realigned PSD traces show a clear aligment. (b) The round 10 correlation attack is successful with 5000 traces.

To ensure that the result was not just due to the filtering effect of the PSD processing, the experiment was repeated, but this time without carrying out the realignment step. As illustrated in Fig. 8 (b), the correlation was unsuccessful after 5000 traces.

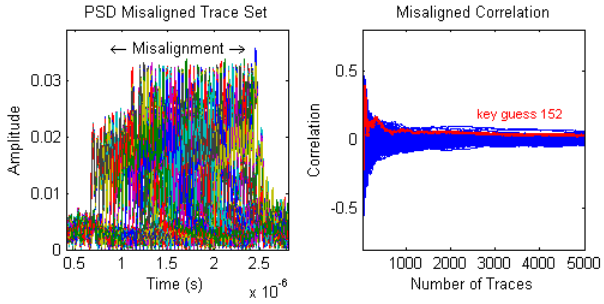

Figure 8. (a) The 5000 traces after PSD processing, but without alignment. (b) The correlation attack is unsuccessful

B. *Encryption Signature Extraction for Cartography*

The analysis was extended further by undertaking a cartography analysis of the Virtex-II FPGA chip of the SASEBO-G. A set of traces was acquired, scanning across the entire chip surface using a Rohde&Schwarz H 2,5-2 magnetic field probe [16]. A grid of 20 mm x 20 mm was covered with a resolution of 1mm per step and a trace recorded at each location.

The traces were then processed through the phase-sensitive detector algorithm, with the reference frequency set at 12 MHz and the low pass filter stop set at 24 MHz, to enhance the peaks as shown in Fig. 9 (b). A threshold level was determined by inspection of Fig. 9 (b) at amplitude of 0.5. The traces, where the width between the two prominent peaks was with ± 10% of Fig. 9 (b), were deemed to match the encryption signature and were therefore identified as containing a detectable pattern. The selection of traces was automated with a simple comparison script in MATLAB, using the above parameters.

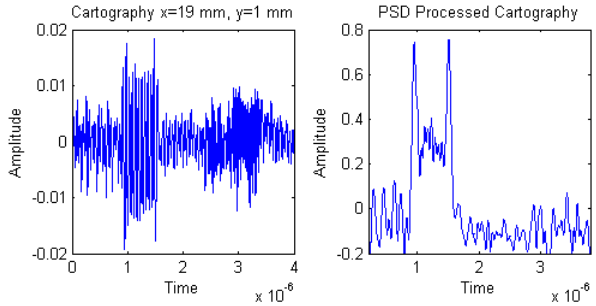

Figure 9. The PSD was used to extract the two-peak characteristic signature shown in (b). The peaks identify the 1st round and data output operations.

The results were plotted in Fig. 10, which uses the dots to illustrate where the encryption signature was detected. This differs from the work of Sauvage *et al.* [17], where only areas of self-similar signals are found, which may or may not be encryption related emanations. In this work we identify the cartography locations where the encryption signal is detectable through our PSD processing, determining the positions where it will be advantageous to gather power traces and mount side-channel analysis with increased efficiency and confidence.

It is interesting to note that the encryption algorithm pattern was detected across the FPGA's entire package area, whereas little was detected in the central core area. This implies detection is coming primarily from the I/O pins of the Virtex-II Pro which are at a 3.3V level, compared to the core at 1.5V.

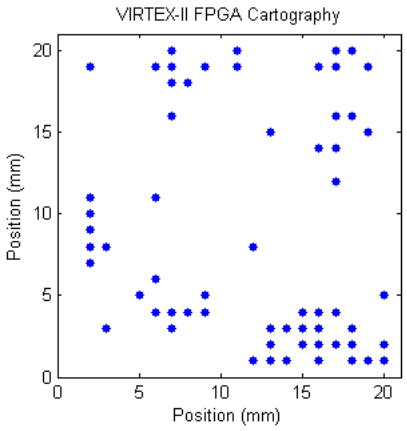

Figure 10. The cartography attack results. The dots represent locations where the encryption signature was detected.

V. CONCLUSIONS & FUTURE WORK

In this work we have introduced a novel application of the phase-sensitive detector in the extraction of characteristic signatures from side channel measurements and shown that this can be used for the purposes of re-alignment and for successful correlation attacks. We have also applied this pre-processing technique to distinguish optimal locations to perform electro-magnetic attacks in conjunction with side-channel cartography.

Interesting future work could be the use of an analog phase-sensitive detector. As the signal processing in the analysis was undertaken post oscilloscope sampling, extra quantization noise was introduced with the oscilloscope's vertical resolution having to cover a larger range due to the high-frequency noise. An analogue phase-sensitive detector circuit could be constructed to pre-process and amplify the waveforms prior to acquisition, which should reduce the quantization noise. This should in turn lead to a greater SNR and key recovery in fewer traces.

REFERENCES

[1] P. C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems." in Advances in Cryptology – CRYPTO '96, Springer, LNCS 1109, pp. 104-113.

[2] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," in Advances in Cryptology – CRYPTO'99, Springer, LNCS 1666, pp. 388-397

[3] J.J. Quisquater, D. Samyde. "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards," In Smart Card Programming and Security (E-smart 2001), LNCS 2140, pp.200-210.

[4] K. Gandolfi, C. Mourtel and F. Olivier. "Electromagnetic Attacks: Concrete Results," in CHES '01, LNCS 2162, pp 251-261.

[5] D. Agrawal, B. Archambeault, J. R. Rao, P Rohatgi. "The EM Side-Channel(s)," in CHES 2002, August 13-15, 2002.

[6] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in CHES 2004, LNCS 3156, 2004, pp. 16-29.

[7] "FIPS PUB 197: the official AES standard," http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[8] N. Homma, S. Nagashima, Y. Imai, T. Aoki, A. Satoh. "High-resolution sidechannel attack using phase-based waveform matching," in CHES 2006. pp187–200.

[9] C. Gebotys and B. White. A phase substitution technique for DEMA of Embedded Cryptographic systems. ITNG, pages 868-869, 2007.

[10] P. Hodgers, K. H. Boey, M. O'Neill. "Variable Window Power Spectral Density Attack" WIFS'2011.

[11] A. Barenghi, G. Pelosi, and Y. Teglia. Improving 1st order dfferential power attacks through digital signal processing. In ACM-SIGSAC International Conference on Security of Information and Networks, pages 124-133. ACM, 2010.

[12] L. Sauvage, S. Guilley, Y. Mathieu, "Electromagnetic radiations of FPGAs: high spatial resolution cartography and attack of a cryptographic module", ACM Transactions on Reconfigurable Technology and Systems (TRETS), Vol. 2, Issue 1, March 2009

[13] ISO/IEC 61967-3: Integrated circuits-Measurement of electromagnetic emissions, 150 kHz to 1 GHz - Part 3: Measurement of radiated emissions – Surface scan method.

[14] Stanford Research Systems, "About Lock-In Amplifiers" www.thinksrs.com/downloads/PDFs/ApplicationNotes/AboutLIAs.pdf

[15] "SASEBO Quick Start Guide," version 1.0, October, 2008, http://www.morita-tech.co.jp/SAKURA/en/index.html

[16] Data Sheet for "R&S HZ-15 E & H near Field Measurements" http://www.rohde-schwarz.co.uk/file_6010/HZ-15_en.pdf

[17] L Sauvage, S Guilley, F Flament "Blind Cartography for Side Channel Attacks: Cross Correlation Cartography". International Journal of Reconfigurable Computing. Volume 2012, Article ID 36.

[18] D. Oswald, C. Paar: Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. CHES 2011. LNCS, vol. 6917, pp. 207–222. Springer, Heidelberg 2011.

[19] C. Clavier, J.-S. Coron, N. Dabbous, "Differential Power Analysis in the presence of Hardware Countermeasures", *Proc. of CHES '00*, Springer LNCS vol. 1965, pp. 252–263, 2000.

[20] A. Moradi, M. Kasper, C. Paar, "Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures – An Analysis of the Xilinx Virtex-4 and Virtex-5 Bitstream Encryption Hardware", CT-RSA 2012, Springer LNCS vol 7178, pp. 1-18, 2012

[21] S. Mangard, E. Oswald, T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards,", 2007, Springer, Verilag. pp 209-211.

[22] Franois Durvaux, Mathieu Renauld, Franois-Xavier Standaert, Loic van Oldeneel tot Oldenzeel, and Nicolas Veyrat-Charvillon. Cryptanalysis of the ches 2009/2010 random delay countermeasure. Cryptology ePrint Archive, Report 2012/038, 2012. http://eprint.iacr.org/.